REMARKS/ARGUMENTS

In the Office action dated March 14, 2005, all of the pending claims were rejected. Claims 1, 5 - 9, 11 - 13, 17 - 21, 23, 24, 31, 32, 36, 37, 44 and 45 were rejected under 35 U.S.C. § 102. Claims 2 - 4, 10, 14 - 16, 22, 25 - 30, 33 - 35 and 38 - 43 were rejected under 35 U.S.C. § 103.

By this Amendment, Applicant has corrected typographical errors in claims 13, 24 and 37 and the Specification. Applicant submits that no new matter has been added by these amendments. Reconsideration and reexamination are hereby requested for claims 1 - 45 that are pending in this application.

Applicant's Response to the Section 102 Rejections

Claims 1, 5 - 9, 11 - 13, 17 - 21, 23, 24, 31, 32, 36, 37, 44 and 45 were rejected under 35 U.S.C. § 102 as being anticipated by Matthews, Jr., U.S. Patent No. 6,549,622 (referred to hereafter as "Matthews"). Claims 1, 13, 24 and 37 are independent.

Applicant respectfully submits that Matthews does not disclose all of the limitations of either of independent claims 1 or 13. Claim 1 recites, in part: "performing a plurality of read data operations and a plurality of write data operations associated with generating the stream cipher in a single cycle." Claim 13 recites, in part: "a plurality of read data operations and the plurality of write data operations associated with generating the stream cipher are performed in a single cycle."

Matthews does not teach or disclose that an accelerator or memory as claimed in claim 1 or claim 13 should or could perform

a plurality of write operations in a single cycle. Rather, Matthews discloses at column 7, lines 56 - 59 that "as shown in table 4, it is possible to perform two "load" operations, an "add" operation and a "store" operation in the same cycle." Thus, Matthews discloses the use of one write operation. Accordingly, Matthews does not anticipate claim 1 or claim 13.

Applicant respectfully submits that Matthews does not disclose all of the limitations of either of independent claims 24 or 37. First, Matthews does not disclose pipelined generation of a key stream byte. Matthews discusses in Tables 3 and 4 techniques for performing multiple operations during a given cycle. However, Matthews does not state that pipelining is possible. Matthews does not even mention the word pipelining anywhere in the specification.

Moreover, the sections of Matthews cited by the Examiner do not teach or suggest the three clock cycle technique claimed in claim 24 and claim 37. The first cycle involves: "incrementing a first address." The third cycle involves: "reading a third memory value at the third address."

The second cycle involves several operations:

reading a first memory value at the first address,

reading a second memory value at a second address obtained by adding the memory value at the first address to a previous second address,

writing the first memory value to the second address and the second memory value to the first address, and

summing the first and second memory values to yield a third address.

In contrast, column 3 of Matthews refers to a seven step method (steps a - g). Here, steps b and c are performed simultaneously. In addition, steps d and e are performed simultaneously. Finally, steps f and g are performed simultaneously. As best understood, the Examiner cites steps b - e as teaching the second cycle of claim 24 and claim 37. These steps, however, refer to two different cycles. When Matthews refers to steps that may occur concurrently, he states that the operation of a step is performed "substantially simultaneously" with another step. The absence of such language with regard to steps b/c and d/e indicates that these steps are not performed in a single cycle.

This interpretation is further supported by Tables 3 and 4 in Matthews. Here, Matthews identifies two different four cycle operations and describes the operations that occur during a given cycle.

The cycles taught by Table 3 of Matthews are not the cycles of claim 24 or claim 37. For example, cycle 3 in Table 3 involves one load, one add and one write. Cycle 4 in Table 3 involves one load, one write and one increment.

The cycles taught by Table 4 of Matthews are not the cycles of claim 24 or claim 37. Cycle 3 in Table 4 involves one load, one add, one write and one increment. Cycle 4 in Table 4 involves two loads, one add and one write.

The discussion at column 12 of Matthews cited by the Examiner also fails to teach or suggest the cycles of claim 24 or claim 37. This discussion relates to Figures 7, 8A and 8B. However, Matthews states that Figure 7 describes a state machine

for implementing the systems of Figures 8A and 8B and that Figures 8A and 8B are a hardware implementation of the method of Table 3. See column 11 at lines 35 - 37 and lines 64 - 66. However, as discussed above, the method of Table 3 does not teach or suggest the cycles of claim 24 or claim 37. Accordingly, Matthews does not anticipate claim 24 or claim 37.

Dependent claims 5 - 9, 11, 12, 17 - 21, 23, 31, 32, 36, 44 and 45 also are patentable over the cited references for the reasons set forth above. In addition, these dependent claims are patentable over these references for the additional limitations that these claims contain.

Response to the § 103 Rejections of the Claims

The Examiner rejected claims 2 - 4, 10, 14 - 16, 22, 25 - 30, 33 - 35 and 38 - 43 under 35 U.S.C. § 103(a) as being unpatentable over various combinations of Matthews; an article by Kundarewich et al. (hereafter referred to as "Kundarewich"); Correale, Jr., U.S. Patent No. 4,998,221; Koppala, U.S., Patent No. 6,289,418; and section 17.1 of the "Applied Cryptography" text. All of the rejected claims are dependent claims. As best understood, all of the rejections under 35 U.S.C. § 103(a) are based on the assertion that Matthews discloses all of the limitations of the base independent claims (claims 1, 13, 24 are 37).

As discussed above, Matthews does not teach or disclose that an accelerator or memory as claimed in claim 1 or claim 13 should or advantageously could perform a plurality of write operations in a single cycle. Moreover, there was no motivation

to modify Matthews in a manner that provides the limitations of these independent claims.

The failure of Matthews to teach or suggest a plurality of write operations in a single cycle is further evidenced by the lack of any discussion in Matthews that indicates or otherwise suggests that Matthews contemplated the problems that could be associated with such multiple writes. In contrast, Applicant teaches coherency checking techniques for handling such problems. See, for example, claims 2 and 29.

None of the other references teach or suggest that multiple writes could be or even should be incorporated into a key stream generation core and/or associated memory as claimed. For example, Kundarewich discloses the conventional technique of RC4 processing where reads and writes are performed sequentially in multiple cycles. As Kundarewich states at page 398, column 2, paragraph 2: "two reads and two writes are necessary for each of the 256 iterations. These reads and writes to RAM define the number of clock cycles possible with the algorithm and hence the minimum number of states." Also see, page 399, column 1: "In each iteration, the values Si and Sj are swapped. This takes four cycles" and the state diagram of Figure 4 that shows that the read and write operations (Read/Write Si/Sj) are performed sequentially.

Moreover, Kundarewich does not teach or suggest the use of coherency checking. Rather, Kundarewich merely teaches that when using the conventional sequential approach the writes must be performed in a particular order "to preserve the coherence of data." Kundarewich at page 398, column 2, paragraph 3. Given

that coherency is thus built into the system of Kundarewich, there is no teaching or suggestion of any need for a system that checks for coherency.

Kundarewich simply discloses the conventional approach disclosed in the Background section of Applicant's specification. For example, at page 1, line 23 - page 2, line 2, Applicant notes that "ARC4 operations are typically performed in strict sequence" and that "to generate a single byte of key stream using ARC4, three reads and two writes to a memory are required," such that "it takes 5 cycles to generate a single byte of data."

In summary, Kundarewich says nothing regarding multiple reads and writes in a single cycle. Likewise Kundarewich says nothing regarding any coherency checking that could be performed in a system that employed such reads and writes.

Furthermore, Correale, Jr. and Koppala are directed to specific memory structures. For example, Correale, Jr. relates to a structure for handling a write through read operation. Correale, Jr. does not teach or suggest how to handle separate read operations and write operations. Koppala relates to a stack management unit. These references do not include any teaching or suggestions relating to whether and how a key stream generation core and/or associated memory could or should be modified.

In view of the above, Applicant submits that independent claims 1 and 13 are not obvious in view of the cited references. It follows that claims 2 - 4, 10, 14 - 16 and 22 that depend on

either claim 1 or claim 13 are patentable over the cited references.

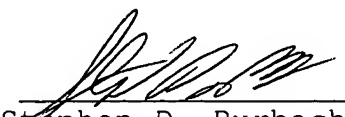
With regard to independent claims 24 and 37, as discussed above in conjunction with Applicant's response to the rejection under 35 U.S.C. § 102, Matthews does not teach or suggest the claimed three cycle technique. Matthews simply teaches a specific four cycle structure for RC4 processing. As discussed above, this structure is significantly different than the claimed three cycle technique. Moreover, Matthews says nothing that would suggest that the claimed technique could or should be implemented nor does Matthew provide any suggestion as to how such a technique could be implemented.

In view of the above, Applicant submits that independent claims 24 and 37 are not obvious in view of the cited references. It follows that claims 25 - 30, 33 - 35 and 38 - 43 that depend on either claim 24 or claim 37 are patentable over the cited references.

CONCLUSION

For the foregoing reasons Applicant submits that the claims are patentable over the references of record. Reexamination and reconsideration are respectfully requested.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By 
Stephen D. Burbach
Reg. No. 40,285
626/795-9900

SDB/vsj
SDB PAS615213.1-*-06/14/05 5:06 PM